D-1150 DIV

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In Re Application of:
Richard A. Steinmetz, et al.

Serial No.: **10/648,936**

Confirm. No.: **5940**

Filed: **August 27, 2003**

For: **Automated Banking Machine Configuration System and Method**

Art Unit
3624

Patent Examiner
Lalita M. Hamilton

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF OF APPELLANTS PURSUANT TO 37 C.F.R. § 41.37

Sir:

The Appellants hereby submit their Supplemental Appeal Brief pursuant to 37 C.F.R. § 41.37 concerning the above-referenced Application.

(i) REAL PARTY IN INTEREST

The Assignee of all right, title and interest to the above-referenced Application is Diebold, Incorporated, an Ohio corporation.

(ii) RELATED APPEALS AND INTERFERENCES

Appellants, Appellants' legal representative, and the assignee of the present application are not aware of any other prior and pending appeals, interferences or judicial proceedings which may be related to, directly affect or have a bearing on the Board's decision in the pending appeal.

(iii) STATUS OF CLAIMS

Claims 13-24 and 28-34 are pending in the Application.

Claims rejected:	13-24 and 28-34
Claims allowed:	none
Claims confirmed:	none
Claims withdrawn:	none
Claims objected to:	none
Claims canceled:	1-12 and 25-27

Appellants appeal the rejections of claims 13-24 and 28-34. These claim rejections were the only claim rejections present in the Office Action ("Action") dated April 24, 2006, which re-opened prosecution after Appellants' first appeal to the Board. Claims 13-24 and 28-34 have been rejected at least twice.

(iv) STATUS OF AMENDMENTS

A non-final rejection was made April 24, 2006. No amendments to the claims were requested to be admitted after the non-final rejection.

(v) SUMMARY OF CLAIMED SUBJECT MATTER

Concise explanations of exemplary forms of the claimed invention:

With respect to independent claim 13

An exemplary form of the invention is directed to a method for configuring an automated banking machine (146) (Figure 6). As discussed in the Specification at page 1, line 10, to page 2, line 2, a common type of automated banking machine is an automated teller machine ("ATM") which enables customers to carry out banking transactions. Common banking transactions that may be carried out with ATMs include the dispensing of cash, the receipt of deposits, the transfer of funds between accounts, the payment of bills and account balance inquiries.

The method comprises a step (a) of receiving a certificate (150, 160) (Figures 6 and 7) through operation of the banking machine (Page 5, line 21, to page 6, line 2; page 17, line 20, to page 18, line 5). Examples discussed in the Specification for this step include loading the certificate on the ATM (146) from a portable storage medium such as a floppy disk, CD-ROM, or card (Figure 6; Page 24, lines 13-14). The Specification also discusses that a certificate (150) may further be downloaded through a network connection from the licensing authority (140) or from some other networked database or storage device (Page 24, lines 14-16).

The method further comprises a step (b) of authenticating at least one digital signature associated with the certificate through operation of the banking machine (page 12, lines 6-11). Examples discussed in the Specification for this step include configuration software (148) operating the ATM (146) which is operative to authenticate the certificate (150) using digital signature authentication techniques (Page 24, line 17, to page 25, line 5).

In addition, the method comprises a step (c) of configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b) (page 25, lines 5-7). Configuration examples discussed in the Specification include configuring which ATM software components among a plurality of software components may be installed on the ATM. Configuring the ATM may also include configuring ATM software, ATM hardware devices, and stored ATM values or other data stored at the ATM (Page 25, line 17, to page 26, line 12).

With respect to independent claim 24

Another exemplary form of the invention is directed to computer readable media bearing instructions (148) (Figure 6) which are operative to cause a computer in an automated banking machine (146) to carry out method steps. As discussed in the Specification at page 1, line 10, to page 2, line 2, a common type of automated banking machine is an automated teller machine ("ATM") which enables customers to carry out banking transactions. Common banking transactions that may be carried out with ATMs include the dispensing of cash, the receipt of deposits, the transfer of funds between accounts, the payment of bills and account balance inquiries.

Such method steps include a step (a) of receiving a certificate (150, 160) (Figures 6 and 7) through operation of the banking machine (Page 5, line 21, to page 6, line 2; page 17, line 20, to page 18, line 5). Examples discussed in the Specification for this step include loading the certificate on the ATM (146) from a portable storage medium such as a floppy disk, CD-ROM, or card (Figure 6; Page 24, lines 13-14). The Specification also discusses that a certificate (150) may further be downloaded through a network connection from the licensing authority (140) or from some other networked database or storage device (Page 24, lines 14-16).

The method further comprises a step (b) of authenticating at least one digital signature associated with the certificate through operation of the banking machine (page 12, lines 6-11). Examples discussed in the Specification for this step include configuration software (148) operating the ATM (146) which is operative to authenticate the certificate (150) using digital signature authentication techniques (Page 24, line 17, to page 25, line 5).

In addition, the method comprises a step (c) of configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b) (page 25, lines 5-7). Configuration examples discussed in the Specification include configuring which ATM software components among a plurality of software components may be installed on the ATM. Configuring the ATM may also include configuring ATM software, ATM hardware devices, and stored ATM values or other data stored at the ATM (Page 25, line 17, to page 26, line 12).

With respect to independent claim 28

Another exemplary form of the invention is directed to a method for configuring a cash dispensing automated teller machine (ATM) (10, 148) (Figures 1, and 6). As discussed in the Specification at page 1, line 10, to page 2, line 2, an ATM enables customers to carry out banking transactions. Common banking transactions that may be carried out with ATMs include the dispensing of cash, the receipt of deposits, the transfer of funds between accounts, the payment of bills, and account balance inquiries.

The method steps include a step (a) of receiving at least one digitally signed certificate (150, 160) (Figures 6 and 7) through operation of the ATM (Page 5, line 21, to page 6, line 2; page 17, line 20, to page 18, line 5). Examples discussed in the Specification for this step include loading the certificate on the ATM (146) from a portable storage medium such as a floppy disk, CD-ROM, or card (Figure 6; Page 24, lines 13-14). The Specification also discusses that a certificate (150) may further be downloaded through a network connection from the licensing authority (140) or from some other networked database or storage device (Page 24, lines 14-16).

In addition, the method is directed to an ATM which includes a cash dispenser (20) and at least one processor. In addition, the method is directed to at least one certificate which includes at least one serial number (Page 26, line 10) which is also referred to in the Specification as a hardware embedded value.

The method further comprises a step (b) of verifying through operation of the at least one processor that the at least one serial number or hardware embedded value included in the at least one certificate corresponds to at least one serial number or hardware embedded value associated with at least one hardware device of the ATM (Page 27, 19 to page 28, line 1).

In addition, the method comprises a step (c) of, responsive to step (b), configuring the ATM through operation of the at least one processor responsive to the at least one digital certificate (Page 28, 1-2). Configuration examples discussed in the Specification include configuring which ATM software components among a plurality of software components may be installed on the ATM. Configuring the ATM may also include configuring ATM software, ATM hardware devices, and stored ATM values or other data stored at the ATM (Page 25, line 17 to page 26, line 12).

(vi) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds to be reviewed in this appeal are:

Whether Appellants' claims 13-24 and 28-34 are anticipated under 35 U.S.C. § 102(e) by Dulude, et al., U.S. Patent No. 6,310,966 ("Dulude").

(vii) ARGUMENT

Dulude

Dulude is directed to a system that authenticates user transactions using biometrics in combination with digital certificates (Column 3, lines 39-50). The system includes biometric certificates (16) which include biometric data (20) therein (Figure 2). The biometric data is pre-stored as biometric certificates in a biometric database (66) of a biometric certificate management system by receiving data corresponding to physical characteristics of registered users through a biometric input device (26) (Figure 3). Subsequent transactions to be conducted over a network (60) have transaction biometric data (46) generated from the physical characteristics of the current user, which transaction biometric data is then appended to transaction first data (50). The transaction is authenticated by comparing the physical characteristics of the current user against the pre-stored biometric data of the physical characteristics of users in the biometric database (Figures 4 and 5).

A second classifier (84) generates a decision in the form of a second validation signal (86), which may be a logic value indicating verification of the authenticity of the user sending the electronic transaction. The second validation signal may also be a numeric value corresponding to a percentage of confidence of authenticity (Figure 5, Column 7, lines 58-67). A receiving section (42) may respond to the validation signals (82, 86) to process the transaction first data (50) such as an on-line purchase or an electronic funds transfer (Column 8, lines 1-7).

Although Dulude mentions that ATMs may access the memory of a smart card to obtain a biometric certificate of a user (Column 5, lines 45-49), Dulude does not teach how ATMs use such certificates. Dulude only discloses using certificates to authenticate user transactions.

Thus, Dulude may arguably suggest that an ATM obtain a biometric certificate of a user for purposes of authenticating user transactions. However, nowhere does Dulude disclose or suggest any other use for biometric certificates other than to authenticate user transactions. As will be discussed below in more detail, Appellants' claims are not directed to using certificates to authenticate user transactions. Rather, Appellants' claims are directed to using certificates to configure an automated banking machine such as an ATM. Nowhere does Dulude disclose or suggest using its biometric certificates or any other type of certificates to configure an automated banking machine, an ATM or any other machine.

The 35 U.S.C. § 102 (e) Rejections

The Applicable Legal Standards

Anticipation pursuant to 35 U.S.C. § 102 requires that a single prior art reference contain all the elements of the claimed invention arranged in the manner recited in the claim. *Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 U.S.P.Q. 193, 198 (Fed. Cir. 1983).

Anticipation under 35 U.S.C. § 102 requires in a single prior art disclosure, each and every element of the claimed invention arranged in a manner such that the reference would literally infringe the claims at issue if made later in time. *Lewmar Marine, Inc. v. Barient, Inc.*, 827 F.2d 744, 747, 3 U.S.P.Q. 2d 1766, 1768 (Fed. Cir. 1987).

Anticipation by inherency requires that the Patent Office establish that persons skilled in the art would recognize that the missing element is necessarily present in the reference. To establish inherency the Office must prove through citation to prior art that the feature alleged to be inherent is "necessarily present" in a cited reference. Inherency may not be established based on probabilities or possibilities. It is plainly improper to reject a claim on the basis of 35 U.S.C. § 102 based merely on the possibility that a particular prior art disclosure could or might be used or operated in the manner recited in the claim. *In re Robertson*, 169 F.3d 743, 49 U.S.P.Q. 2d 1949 (Fed. Cir. 1999).

It is respectfully submitted that the Action from which this appeal is taken does not meet these burdens.

Rejection under 35 U.S.C. § 102(e) over Dulude

Claims 13-24 and 28-34 were rejected under 35 U.S.C. § 102(e) as being anticipated by Dulude. These rejections are respectfully traversed.

Claim 13

Claim 13 is an independent claim directed to a method for configuring an automated banking machine. The method comprises: (a) receiving a certificate through operation of the banking machine; (b) authenticating at least one digital signature associated with the certificate through operation of the banking machine; and (c) configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b).

The Action states that Dulude discloses configuring the banking machine responsive to the certificate and authentication of the at least one digital signature at: Column 1, line 65-column 2, line 15; Column 3, lines 28-50; Column 5, lines 33-50; and Column 8, lines 34-45.

Appellants disagree. Nowhere do these portions of Dulude nor any other portion of Dulude disclose or suggest these features. For example, claim 13 recites "configuring the banking machine responsive to the certificate". Nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to a certificate. Dulude is directed to a system that authenticates transactions using biometric certificates. Although Dulude states that ATMs may access a memory (66) to obtain a secured biometric certificate of a user, nowhere does Dulude disclose or suggest that its biometric certificates are ever used by an automated banking machine to configure the automated banking machine.

In Dulude, authentication of a transaction is carried out by comparing the physical (biometric) characteristics of a user initiating the transaction against pre-stored biometric data in a biometric certificate (Column 3, lines 30-50). Dulude does not disclose or suggest using certificates to configure an automated banking machine. Further, nowhere does Dulude disclose or suggest any feature or data in its biometric certificates that is capable of being used to configure an automated banking machine.

In addition, claim 13 specifically recites configuring the banking machine responsive to the certificate <u>and</u> authentication of the at least one digital signature associated with the certificate. Nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to <u>both</u> a digital certificate and authentication of a digital signature associated with the certificate. At best, Dulude only shows authenticating a transaction using data in biometric digital certificate. Thus, Dulude does not disclose or suggest **configuring an automated banking machine responsive to a certificate and authentication of at least one digital signature** associated with the certificate, as specifically recited in step (c) of claim 13.

Further, nowhere does Dulude disclose or suggest a step of authenticating at least one digital signature associated with the certificate through operation of the banking machine. In Dulude, a transaction system (40) (Figure 4) may be used to acquire transaction biometric data (46) from a first user and generate transaction first data (50). Such transaction first data may be an electronic funds transfers through an ATM (Column 5, lines 50-62). A digital signature function (54) is then used to generate (not authenticate) a digital signature (58) from a hash of the transaction first date and biometric data. (Column 6, lines 1-17). This digital signature (58) is then sent to a network (60) where it is received by a receiving section (42) (Figure 5; Column 6, lines 28-30). Authentication of the digital signature is carried out by the receiving station (Column 7, lines 4-25).

Thus Dulude only shows authenticating a digital signature associated with transaction data and biometric data. Nowhere does Dulude disclose or suggest Appellants' recited step of authenticating at least one digital signature **associated with the certificate**. Further, nowhere does Dulude disclose an automated banking machine that operates to authenticate a digital signature associated with a certificate, as specifically recited by Appellants.

Dulude does not explicitly or inherently teach all the recited features, relationships, and steps. For all of these many reasons Dulude does not anticipate claim 13. Therefore, Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection should be reversed.

Claim 14

Claim 14 depends from claim 13 and recites that in step (a) the certificate includes the digital signature. Claim 14 also recites that in step (b) the digital signature is authenticated responsive to a public key of a licensing authority.

Dulude does not disclose or suggest these features. Dulude does not disclose or suggest authenticating a digital signature included in a certificate. Further, nowhere does Dulude disclose or suggest a digital signature that is authenticated responsive to a public key of a licensing authority. As discussed previously, the only digital signature (58) that is authenticated in Dulude is associated with transaction data and biometric data, not a digital certificate. In addition, Dulude specifically teaches that this digital signature (58) is decrypted using **a user public key** (74) (Column 6, lines 66-67). Nowhere does Dulude disclose or suggest authenticating a digital signature using a public key of a licensing authority. In addition, nowhere does Dulude disclose or suggest authenticating a digital signature included in a certificate **through operation of an automated banking machine**. Dulude does not explicitly or inherently teach this feature and therefore does not anticipate claim 14. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 14 should be reversed.

Claim 15

Claim 15 depends from claim 13 and recites that in step (a) the certificate corresponds to at least one software component authorized to be installed on the banking machine. Claim 15 also recites that the method further comprises installing the at least one software component on the banking machine.

With respect to these features, the Action points to: Column 1, line 65, to column 2, lines 15; Column 3, lines 28-50; Column 5, lines 33-50; and Column 8, lines 34-45 of Dulude. However, nowhere in these cited portions nor anywhere else does Dulude disclose or suggest the features, relationships and steps recited in claim 15. As discussed previously, Dulude uses biometric certificates to authenticate transactions. Nowhere does Dulude disclose or suggest a certificate that **corresponds to at least one software component**. In addition, nowhere does Dulude disclose or suggest a certificate that corresponds to at least one software component **authorized to be installed on the banking machine**. Further, nowhere does Dulude teach or suggest the step of **installing the at least one software component on the banking machine,** which at least one software component corresponds to a digital certificate. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 15. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 15 should be reversed.

Claim 16

Claim 16 depends from claim 13 and recites that in step (a) the certificate includes a plurality of sets of configuration rules. Each set corresponds to at least one of a plurality of automated banking machines. Claim 16 also recites that in step (c) the banking machine is enabled to be configured responsive to at least one set.

Dulude does not disclose or suggest these recited features, relationships and steps. In Dulude, a biometric certificate is generated from a set (16) of data that includes a subject unique ID (18), and biometric data (20) (Column 4, lines 7-8). Nowhere does Dulude disclose or suggest a certificate which includes **a plurality of sets of configuration rules**. Further, nowhere does Dulude disclose or suggest that each set of configuration rules corresponds **to at least one of a plurality of automated banking machines**. In addition, nowhere does Dulude disclose or suggest that an automated banking machine **is enabled to be configured responsive to at least one set** of the configuration rules included in a digital certificate. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 16. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 16 should be reversed.

Claim 17

Claim 17 depends from claim 13 and recites that the certificate further includes an expiration parameter. Claim 17 also recites that the method includes (d) determining through operation of the banking machine responsive to the expiration parameter that configuration of the software on the machine is not authorized. In addition, claim 17 recites that the method includes (e) preventing configuration of software on the banking machine responsive to the determination in step (d).

Dulude does not disclose or suggest these recited features, relationships and steps. In Dulude, authenticating certificates may be generated by concatenating a message and a public key with a set of data which may include an expiration of validity of the certificate (Column 1, line 66, to column 2, line 13). However, nowhere does Dulude disclose or suggest determining, through operation of an automated banking machine responsive to the expiration parameter in a certificate, **that configuration of the software on the machine is not authorized**. In addition, Dulude does not disclose or suggest determining through operation of an automated banking machine **responsive to the expiration parameter** in a certificate that configuration of software on the machine is not authorized. Further, nowhere does Dulude disclose or suggest **preventing configuration of software on the banking machine**. In addition, nowhere does Dulude disclose or suggest preventing configuration of software on the banking machine **responsive to the determination** that configuration of software on the machine is not authorized. As Dulude does not explicitly or inherently teach these features, Dulude does not anticipate claim 17. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 17 should be reversed.

Claim 18

Claim 18 depends from claim 13 and recites that in step (a) the certificate includes an identification value unique to the banking machine. Dulude does not disclose or suggest these recited features.

In Dulude, authenticating certificates may be generated by concatenating a message and a public key with a set of data which may include an issuer unique ID number and a subject unique ID number (12) (Column 1, line 66, to column 2, line 13). The subject unique ID number is described as corresponding to a Social Security number or a password associated with the user sending the transaction. However, nowhere does Dulude disclose or suggest that such IDs correspond to **an identification value unique to the banking machine**. As Dulude does not explicitly or inherently teach this feature, Dulude does not anticipate claim 18. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 18 should be reversed.

Claim 19

Claim 19 depends from claim 18 and recites that the method further comprises prior to step (c): determining through operation of the banking machine that the identification value corresponds to a hardware embedded identification value in the banking machine. Dulude does not disclose or suggest these recited features. Nowhere does Dulude disclose or suggest a step of determining through operation of a banking machine that an identification value included in a certificate **corresponds to a hardware embedded identification value in the banking machine**. Dulude does not explicitly or inherently teach this feature and therefore does not anticipate claim 19. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 19 should be reversed.

Claim 20

Claim 20 depends from claim 13 and recites that in step (a) the certificate includes a terminal identification value. In addition, claim 20 recites that step (c) includes associating the machine with the terminal identification value. Dulude does not disclose or suggest these recited features, relationships and steps.

Nowhere does Dulude disclose or suggest a certificate which includes **a terminal identification value**. Further, nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to the certificate including **associating the machine with the terminal identification value**. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 20. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 20 should be reversed.

Claim 21

Claim 21 depends from claim 20 and recites that the method further comprises: (d) determining that the terminal identification value has changed; and (e) preventing the machine from performing at least one transaction function responsive to the determination in step (d). Dulude does not disclose or suggest these recited features, relationships and steps.

Nowhere does Dulude disclose or suggest **determining that the terminal identification value** associated with an automated banking machine **has changed**. Further, nowhere does Dulude disclose or suggest **preventing the machine from performing at least one transaction function responsive to the determination** that the terminal identification value has changed. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 21. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 21 should be reversed.

Claim 22

Claim 22 depends from claim 13 and recites that step (a) includes retrieving the certificate from a licensing authority. Dulude does not disclose or suggest these recited features, relationships and steps.

Dulude teaches that ATMs may access a memory of a smart card to obtain biometric certificates of a user (Column 5, lines 45-49). However, nowhere does Dulude disclose or suggest **retrieving the certificate from a licensing authority** through operation of an automated banking machine. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 22. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 22 should be reversed.

Claim 23

Claim 23 depends from claim 13 and recites that step (a) includes receiving the certificate from a server in operative connection with the banking machine. Dulude does not disclose or suggest these recited features, relationships and steps.

Dulude teaches that ATMs may access a memory of a smart card to obtain biometric certificates of a user (Column 5, lines 45-49). However, nowhere does Dulude disclose or suggest **receiving the certificate from a server in operative connection with the banking machine**. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 23. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 23 should be reversed.

Claim 24

Claim 24 is an independent claim directed to computer readable media. The computer readable media bears instructions which are operative to cause a computer in an automated banking machine to carry out the method steps of: (a) receiving a certificate through operation of the banking machine; (b) authenticating at least one digital signature associated with the certificate through operation of the banking machine; and (c) configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b).

The Action states that Dulude discloses configuring the banking machine responsive to the certificate and authentication of the at least one digital signature at: Column 1, line 65-column 2, line 15; Column 3, lines 28-50; Column 5, lines 33-50; and Column 8, lines 34-45. Applicants disagree. Nowhere do these portions of Dulude, nor any other portion of Dulude disclose or suggest these features. For example, claim 24 recites "configuring the banking machine responsive to the certificate". Nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to a certificate. Dulude is directed to a system that authenticates transactions using biometric certificates. Although Dulude states that ATMs may access a memory (66) to obtain a secured biometric certificate of a user, nowhere does Dulude disclose or suggest that its biometric certificates are ever used by an automated banking machine to configure the automated banking machine.

In Dulude, authentication of a transaction is carried out by comparing the physical (biometric) characteristics of a user initiating the transaction against pre-stored biometric data in a biometric certificate (Column 3, lines 30-50). Dulude does not disclose or suggest using certificates to configure an automated banking machine. Further, nowhere does Dulude disclose or suggest any feature or data in its biometric certificates that is capable of being used to configure an automated banking machine.

In addition, claim 24 specifically recites configuring the banking machine responsive to the certificate <u>and</u> authentication of the at least one digital signature associated with the certificate. Nowhere does Dulude disclose or suggest configuring an automated banking machine responsive to <u>both</u> a digital certificate and authentication of a digital signature associated with the certificate. At most, Dulude only shows authenticating a transaction using data in biometric digital certificate. Thus, Dulude does not disclose or suggest Appellants' step (c) of **configuring an automated banking machine responsive to a certificate and authentication of at least one digital signature** associated with the certificate.

Further, nowhere does Dulude disclose or suggest a step of authenticating at least one digital signature associated with the certificate through operation of the banking machine. In Dulude, a transaction system (40) (Figure 4) may be used to acquire transaction biometric data (46) from a first user and generate transaction first data (50). Such transaction first data may be an electronic funds transfers through an ATM (Column 5, lines 50-62). A digital signature function (54) is then used to generate (not authenticate) a digital signature (58) from a hash of the transaction first date and biometric data. (Column 6, lines 1-17). This digital signature (58) is then sent to a network (60) where it is received by a receiving section (42) (Figure 5, Column 6, lines 28-30). Authentication of the digital signature is carried out by the receiving station (Column 7, lines 4-25).

Thus Dulude only shows authenticating a digital signature associated with transaction data and biometric data. Nowhere does Dulude disclose or suggest authenticating at least one digital signature **associated with the certificate** as specifically recited by Appellants. Further, nowhere does Dulude disclose an automated banking machine that operates as specifically recited, to authenticate a digital signature associated with a certificate.

Dulude does not explicitly or inherently teach the recited features, relationships, and steps. For all of these many reasons, Dulude does not anticipate claim 24. Therefore, Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 24 should be reversed.

Claim 28

Claim 28 is an independent claim directed to a method for configuring a cash dispensing automated teller machine (ATM). The method comprises: (a) receiving at least one digitally signed certificate through operation of the ATM. The ATM includes a cash dispenser and at least one processor. The at least one certificate includes at least one serial number. In addition, the method comprises: (b) verifying through operation of the at least one processor that the at least one serial number included in the at least one certificate corresponds to at least one serial number associated with at least one hardware device of the ATM. Also, the method comprises: (c) responsive to (b), configuring the ATM through operation of the at least one processor responsive to the at least one digital certificate. Dulude does not disclose or suggest these recited features, relationships and steps.

Dulude teaches that an authenticating certificate may include a serial number for the certificate with respect to a sequence of generated certificates (Column 2, lines 6-8). However, nowhere does Dulude disclose or suggest a step that involves **verifying through operation of the at least one processor** in the ATM **the at least one serial number included in the at least one certificate**. In addition, nowhere does Dulude disclose or suggest verifying through operation of at least one processor in an ATM **that the at least one serial number included in the at least one certificate corresponds to at least one serial number associated with at least one hardware device of the ATM**. Further, nowhere does Dulude disclose or suggest that any other data included in a certificate corresponds to a serial number associated with an ATM hardware device. Also, nowhere does Dulude disclose or suggest **at least one serial number associated with at least one hardware device of the ATM.**

In addition, claim 28 recites responsive to this verifying step (b), configuring the ATM through operation of the at least one processor in the ATM responsive to the at least one digital certificate. Nowhere does Dulude disclose or suggest configuring an ATM responsive to a digital certificate.

Dulude discusses comparing the physical (biometric) characteristics of a user initiating the transaction against pre-stored biometric data in a biometric certificate. (Column 3, lines 30-50). Thus, in Dulude, biometric certificates are used to authenticate a transaction, not to configure an ATM.

Nowhere does Dulude disclose or suggest **configuring the ATM responsive to the at least one digital certificate**. In addition, Dulude does not disclose or suggest configuring the ATM **through operation of the at least one processor** in the ATM responsive to the at least one digital certificate. Further, nowhere does Dulude disclose or suggest configuring the ATM responsive to a digital certificate and responsive to a step of verifying that a serial number included in the at least one certificate corresponds a serial number associated with at least one hardware device of the ATM.

Dulude does not explicitly or inherently teach the recited features, relationships, and steps. For all of these many reasons, Dulude does not anticipate claim 28. Therefore, Appellants respectfully submit that the 35 U.S.C. § 102(e) of claim 28 rejection should be reversed.

Claim 29

Claim 29 depends from claim 28 and recites that the at least one certificate includes at least one digital signature. Claim 28 also recites that the method further comprises: (d) prior to

(c) authenticating the at least one digital signature through operation of the at least one processor. In addition, claim 29 recites that (c) is carried out responsive to (b) and (d). Dulude does not disclose or suggest these recited features, relationships and steps.

In Dulude, a transaction system (40) (Figure 4) may be used to acquire transaction biometric data (46) from a first user and generate transaction first data (50). Such transaction first data may be an electronic funds transfers through an ATM (Column 5, lines 50-62). A digital signature function (54) is then used to generate (not authenticate) a digital signature (58) from a hash of the transaction first data and biometric data. (Column 6, lines 1-17). This digital signature (58) is then sent to a network (60) where it is received by a receiving section (42) (Figure 5; Column 6, lines 28-30). Authentication of the digital signature is carried out by the receiving station (Column 7, lines 4-25).

Nowhere does Dulude disclose or suggest a step of **authenticating the at least one digital signature** included in a certificate **through operation of the at least one processor** in an ATM. In addition, Dulude does not disclose or suggest configuring an ATM responsive to both: authenticating the at least one digital signature included in the certificate; and verifying that at least one serial number included in the certificate corresponds a serial number associated with an ATM hardware device. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 29. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 29 should be reversed.

Claim 30

Claim 30 depends from claim 29 and recites that (a) includes receiving the at least one certificate from a server in operative connection with the ATM through a network. Dulude does not disclose or suggest these recited features, relationships and steps.

Dulude teaches that ATMs may access a memory of a smart card to obtain biometric certificates of a user (Column 5, lines 45-49). However, nowhere does Dulude disclose or suggest receiving the at least one certificate with the ATM **from a server in operative connection with the ATM through a network**. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 30. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 30 should be reversed.

Claim 31

Claim 31 depends from claim 30 and recites that the at least one hardware device corresponds to at least one of a keypad, a card reader, the cash dispenser, a printer, a depositor, a CPU, and a network device. Dulude does not disclose or suggest these recited features.

Nowhere does Dulude disclose or suggest configuring an ATM responsive to a step (b) of verifying that at least one serial number included in a certificate corresponds to a serial number associated with **at least one of a keypad, a card reader, the cash dispenser, a printer, a depositor, a CPU, and a network device** of an ATM. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 31. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 31 should be reversed.

Claim 32

Claim 32 depends from claim 30 and recites that prior to (c) the ATM is not enabled to perform at least one transaction function involving the operation of the at least one hardware device. Claim 32 further recites that in (c) configuring the ATM includes enabling the ATM to perform the at least one transaction function involving the operation of the at least one hardware device. Dulude does not disclose or suggest these recited features, relationships and steps.

Nowhere does Dulude disclose or suggest that prior to configuring the ATM responsive to the certificate, **the ATM is not enabled to perform at least one transaction function involving the operation of the at least one hardware device**. Further, nowhere does Dulude disclose or suggest that configuring the ATM includes **enabling the ATM to perform the at least one transaction function involving the operation of the at least one hardware device**. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 32. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 32 should be reversed.

Claim 33

Claim 33 includes a typographical error with respect to the claim from which it depends. Claim 33 should depend from claim 32. Upon the resolution of the Appeal, Appellants are willing to correct claim 33 to depend from claim 32.

With respect to the subject matter recited in claim 33, claim 33 recites that in (c) the at least one transaction function includes dispensing cash. Claim 33 further recites that the method comprises (e) dispensing cash from the ATM through operation of the cash dispenser. Dulude does not disclose or suggest these recited features, relationships and steps.

Nowhere does Dulude disclose or suggest that configuring the ATM responsive to a certificate includes enabling the ATM to dispense cash through operation of the cash dispenser in the ATM. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 33. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 33 should be reversed.

Claim 34

Claim 34 depends from claim 30 and recites that (c) includes configuring the ATM responsive to at least one key provided in the at least one certificate. Dulude does not disclose or suggest these recited features, relationships and steps.

Although Dulude discloses a subject public key (Figure 1; Column 1, line 66, to column 2, line 1), nowhere does Dulude disclose or suggest **configuring the ATM responsive to at least one key provided in the at least one certificate**. Dulude does not explicitly or inherently teach these features and therefore does not anticipate claim 34. Appellants respectfully submit that the 35 U.S.C. § 102(e) rejection of claim 34 should be reversed.

CONCLUSION

Each of Appellants' pending claims specifically recites elements, relationships, and steps that are neither disclosed nor suggested in any of the applied prior art. Furthermore, the applied prior art is devoid of any teaching, suggestion, or motivation for producing the recited invention.

For these reasons it is respectfully submitted that all the rejections should be reversed.

Respectfully submitted,

Ralph E. Jocke Reg. No. 31,029
WALKER & JOCKE
231 South Broadway
Medina, Ohio 44256
(330) 721-0000

(viii) CLAIMS APPENDIX

13. A method for configuring an automated banking machine comprising:

a) receiving a certificate through operation of the banking machine;

b) authenticating at least one digital signature associated with the certificate through operation of the banking machine;

c) configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b).

14. The method according to claim 13, wherein in step (a) the certificate includes the digital signature, wherein in step (b) the digital signature is authenticated responsive to a public key of a licensing authority.

15. The method according to claim 13, wherein in step (a) the certificate corresponds to at least one software component authorized to be installed on the banking machine, and further comprising installing the at least one software component on the banking machine.

16. The method according to claim 13, wherein in step (a) the certificate includes a plurality of sets of configuration rules each set corresponding to at least one of a plurality of automated banking machines, and wherein in step (c) the banking machine is enabled to be configured responsive to at least one set.

17. The method according to claim 13, wherein the certificate further includes an expiration parameter, and further comprising:

d) determining through operation of the banking machine responsive to the expiration parameter that configuration of the software on the machine is not authorized; and

e) preventing configuration of software on the banking machine responsive to the determination in step (d).

18. The method according to claim 13, wherein in step (a) the certificate includes an identification value unique to the banking machine.

19. The method according to claim 18, further comprising prior to step (c):

determining through operation of the banking machine that the identification value corresponds to a hardware embedded identification value in the banking machine.

20. The method according to claim 13, wherein in step (a) the certificate includes a terminal identification value, wherein step (c) includes associating the machine with the terminal identification value.

21. The method according to claim 20, further comprising:

d) determining that the terminal identification value has changed; and

e) preventing the machine from performing at least one transaction function responsive to the determination in step (d).

22. The method according to claim 13, wherein step (a) includes retrieving the certificate from a licensing authority.

23. The method according to claim 13, wherein step (a) includes receiving the certificate from a server in operative connection with the banking machine.

24. Computer readable media bearing instructions which are operative to cause a computer in an automated banking machine to carry out the method steps of:

a) receiving a certificate through operation of the banking machine;

b) authenticating at least one digital signature associated with the certificate through operation of the banking machine;

c) configuring the banking machine responsive to the certificate and authentication of the at least one digital signature in step (b).

28. A method for configuring a cash dispensing automated teller machine (ATM) comprising:

a) receiving at least one digitally signed certificate through operation of the ATM, wherein the ATM includes a cash dispenser and at least one processor, wherein the at least one certificate includes at least one serial number;

b) verifying through operation of the at least one processor that the at least one serial number included in the at least one certificate corresponds to at least one serial number associated with at least one hardware device of the ATM;

c) responsive to (b), configuring the ATM through operation of the at least one processor responsive to the at least one digital certificate.

29. The method according to claim 28, wherein the at least one certificate includes at least one digital signature; and further comprising:

d) prior to (c) authenticating the at least one digital signature through operation of the at least one processor;

wherein (c) is carried out responsive to (b) and (d).

30. The method according to claim 29, wherein (a) includes receiving the at least one certificate from a server in operative connection with the ATM through a network.

31. The method according to claim 30, wherein the at least one hardware device corresponds to at least one of a keypad, a card reader, the cash dispenser, a printer, a depositor, a CPU, and a network device.

32. The method according to claim 30, wherein prior to (c) the ATM is not enabled to perform at least one transaction function involving the operation of the at least one hardware device, wherein in (c) configuring the ATM includes enabling the ATM to perform the at least one transaction function involving the operation of the at least one hardware device.

33. The method according to claim 33, wherein in (c) the at least one transaction function includes dispensing cash, wherein further comprising:

e) dispensing cash from the ATM through operation of the cash dispenser.

34. The method according to claim 30, wherein (c) includes configuring the ATM responsive to at least one key provided in the at least one certificate.

(ix) EVIDENCE APPENDIX

(None)

(x) RELATED PROCEEDINGS APPENDIX

(None)